U.S. General Services Administration

GSA Federal Acquisition Training Symposium

May 10-11, 2016
Huntsville, AL

Learn > Discuss > Connect Interact

Navigating Unclassified Information System Security Protections

Network Penetration Reporting and Contracting for Cloud Services

Vicki Michetti, DoD CIO, Director, DIB Cybersecurity Program

Mary Thomas, OUSD(AT&L), Defense Procurement and Acquisition Policy

Outline

- DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services
  - Safeguarding Covered Defense Information (CDI)
    - Adequate Security to Safeguard Covered Defense Information
    - Cyber Incident Reporting
    - Damage Assessment
  - Cloud Computing/Contracting for Cloud Services
- Moving Forward
- Resources

Network Penetration Reporting and Contracting for Cloud Services

DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services, 2nd interim rule effective on December 30, 2015

- Revises the DFARS to implement Section 941 of NDAA for FY13, Section 1632 of NDAA for FY15 (codified at 10 U.S.C. §§ 393 & 391), and DoD policy and procedures for use when contracting for cloud computing services
- Includes 3 clauses and 2 provisions:

Safeguarding Covered Defense Information

- (p) Section 252.204-7008, Compliance with Safeguarding Covered Defense Information → All solicitations/contracts
- (c) Section 252.204-7009, Limitation on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information → Solicitations/contracts for services that support safeguarding/reporting
- (c) Section 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting → All solicitations/contracts

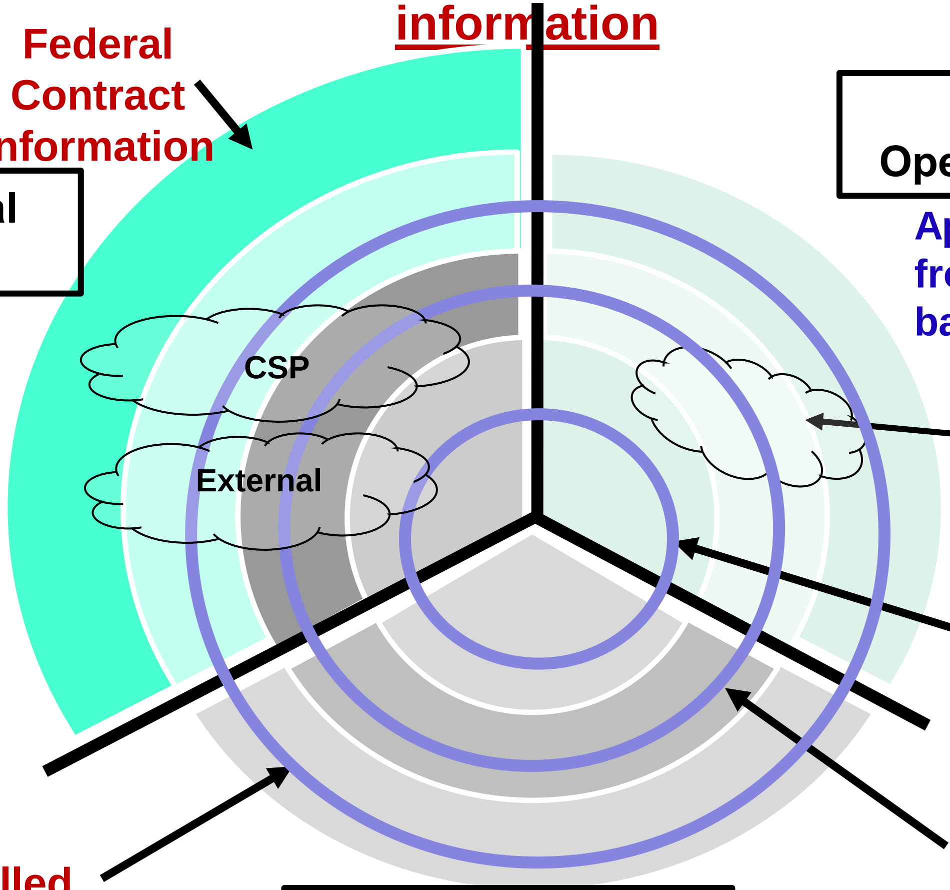
Contracting For Cloud Services

- (p) Section 252.239-7009, Representation of Use of Cloud Computing
- (c) Section 252.239-7010, Cloud Computing Services

→ Solicitations and contracts for IT services

Unclassified Information System Security Protections

Elements that drive appropriate protections: The information system and the information



(ref. FAR Case 2011-020)

Federal Contract Information

Contractor's Internal System

Applicable controls: NIST SP 800-171

Contractor System Operated on DoD's Behalf

Applicable controls: from CNSSI 1253, based on NIST SP 800-53

Cloud Service Provider

Applicable controls: From the SRG

Unclassified Controlled Technical Information

Covered Defense Information

Controlled Unclassified Information (USG-wide)

DoD Information System

Applicable controls: From CNSSI 1253, based on NIST SP 800-53

DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

	Nov 18, 2013 *(Final Rule)*	**Aug 26, 2015 *(Interim Rule)***	**Dec 30, 2015*(Interim Rule)***
Scope – What Information?	• **Unclassified Controlled Technical Information**	• **Covered Defense Information** • **Operationally Critical Support**	• Covered Defense Information • Operationally Critical Support
Adequate Security – What Minimum Protections?	• Selected controls in **NIST SP 800-53**, Security and Privacy Controls for **Federal Information Systems** and Organizations	• **NIST SP 800-171,** Protecting Controlled Unclassified Information on **Nonfederal Information Systems** and Organizations	• NIST SP 800-171, Protecting Controlled Unclassified Information on Nonfederal Information Systems and Organizations
When?	• Contract Award	• Contract Award • **Oct 8, 2015 Deviation** – Security Requirement 3.5.3, **within 9 months of Award**	• As soon as practicable, but **NLT Dec 31, 2017**

- Due to the differences in the multiple versions of DFARS Clause 252.204-7012, amending the contract requires PCO authority and contractor signature (i.e., a bilateral agreement).
- There is nothing however that precludes a Contracting Officer from considering a modification of the contract upon request of the contractor.

What is Covered Defense Information?

Three conditions apply:	
1	Unclassified information that is provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or
	Unclassified information that is collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract;
2	Falls in any of the following categories: – Controlled technical information – Critical information (operations security) – Export control – Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies
3	Is identified in the contract, task order, or delivery order

Network Security Controls to Safeguard Covered Defense Information

DFARS Clause 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting *(effective December 30, 2015)*

(b) To provide adequate security, the Contractor shall—

(1) Implement information systems security protections on all covered contractor information systems including, at a minimum—

(ii) For covered contractor information systems …

(A) The security requirements in NIST SP 800-171 as soon as practical, but not later than Dec 31, 2017.

Compliance

Q: Does the Government intend to monitor contractors to ensure implementation of the required security requirements?

A: The DFARS rule did not add any unique or additional requirement for the Government to monitor contractor implementation of required security requirements. Contractor compliance with these requirements are subject to existing, generally applicable, contractor compliance monitoring mechanisms.

NIST SP 800-171, Protecting CUI in Nonfederal Information Systems and Organizations

- **Developed for use on contractor and other nonfederal information systems to protect CUI *(published June 2015)***
  - **Replaces use of selected security controls from NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations in original DFARS Clause 252.204-7012 *(circa November 18, 2013)***
- **Enables contractors to comply using systems and practices already in place**
  - **Intent is not to require the development or acquisition of new systems to process, store, or transmit CUI**
  - **Requirements are performance-based, significantly reduce unnecessary specificity, and are more easily applied to existing systems.**
- **Provides standardized/uniform set of requirements for all CUI security needs**
  - **Allows nonfederal organizations to consistently implement safeguards for the protection of CUI (i.e., one CUI solution for all customers)**
  - **Allows contractor to implement alternative, but equally effective, security measures to satisfy every CUI security requirement**

Replacing NIST SP 800-53 based controls with NIST SP 800-171

NIST SP 800-171 Requirement	NIST SP 800-53 Requirement (from DFARS Table 1)
3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). **3.1.2** Limit information system access to the types of transactions and functions authorized users are permitted to execute.	**AC-2 ACCOUNT MANAGEMENT The organization:** a. Identifies/selects the following types of information system accounts to support organizational missions/ business functions: [Assignment: organization-defined information system account types]; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]; g. Monitors the use of, information system accounts; h. Notifies account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; i. Authorizes access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group. **AC-3 ACCESS ENFORCEMENT The information system** enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. **AC-17 REMOTE ACCESS The organization:** a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorizes remote access to the information system prior to allowing such connections.

Replacing NIST SP 800-53 based controls with NIST SP 800-171

NIST SP 800-171 Requirement	NIST SP 800-53 Requirement (from DFARS Table 1)
3.8.9 Protect the confidentiality of backup CUI at storage locations.	**CP-9 INFORMATION SYSTEM BACKUP** **The organization:** a. Conducts backups of user-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; b. Conducts backups of system-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; c. Conducts backups of information system documentation including security-related documentation [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; and d. **Protects the confidentiality**, integrity, and availability **of backup** information **at storage locations.**
3.5.5 Prevent reuse of identifiers for a defined period. **3.5.6** Disable identifiers after a defined period of inactivity.	**IA-4 IDENTIFIER MANAGEMENT** **The organization manages information system identifiers by:** a. Receiving authorization from [*Assignment: organization-defined personnel or roles*] to assign an individual, group, role, or device identifier; b. Selecting an identifier that identifies an individual, group, role, or device; c. Assigning the identifier to the intended individual, group, role, or device; d. **Preventing reuse of identifiers for** [*Assignment: organization-**defined** time **period***]; and e. **Disabling the identifier after** [*Assignment: organization-**defined** time **period of inactivity***].

Replacing NIST SP 800-53 based controls with NIST SP 800-171

NIST SP 800-171 Requirement	NIST SP 800-53 Requirement (from DFARS Table 1)
3.10.3 Escort visitors and monitor visitor activity. **3.10.4** Maintain audit logs of physical access **3.10.5** Control and manage physical access devices	**PE -3 PHYSICAL ACCESS CONTROL The organization:** a. Enforces physical access authorizations at [*Assignment: organization-defined entry/exit points to the facility where the information system resides*] by; 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using [*Selection (one or more): [Assignment: organization-defined physical access control systems/devices*]; *guards*]; b. **Maintains physical access audit logs** for [*Assignment: organization-defined entry/exit points*]; c. Provides [*Assignment: organization-defined security safeguards*] to control access to areas within the facility officially designated as publicly accessible; d. **Escorts visitors and monitors visitor activity** [*Assignment: organization-defined circumstances requiring visitor escorts and monitoring*]; **e. Secures keys, combinations, and other physical access devices;** **f. Inventories [*Assignment: organization-defined physical access devices*] every [*Assignment: organization-defined frequency*]; and** **g. Changes combinations and keys [*Assignment: organization-defined frequency*] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.**

Network Security Controls to Safeguard Covered Defense Information

- The contractor shall implement the security requirements in NIST SP 800-171 as soon as practical, but not later than Dec 31, 2017.
- The Contractor shall notify DoD CIO within 30 days of contract award of any security requirements not implemented at the time of contract award;
- If the offeror proposes to vary from NIST SP 800-171, the Offeror shall submit to the Contracting Officer, a written explanation of -
  - Why security requirement is not applicable; or
  - How an alternative but equally effective security measure is used to achieve equivalent protection

DFARS Clause 252.204-7012 (b)(2) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.

Cyber Incident Reporting

DFARS 252.204-7012 (c) Cyber incident reporting requirement.

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support, the Contractor shall—

(i) Conduct a review for evidence of compromise …

(ii) Rapidly report cyber incidents to DoD …

DFARS 252.204-7012 (d) Malicious Software. The Contractor or subcontractors that discover/isolate malicious software… shall submit the malicious software in accordance with instructions provided by the Contracting Officer.

The contracting officer should never receive malicious software directly from the contractor

What is Operationally Critical Support?

- Supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.
  - Operationally Critical Support is an “activity” performed by the contractor.
  - DFARS does not require protections for contractor information systems that are used to provide operationally critical support – the requirement is for the contractor to report a cyber incident that affects the contractor’s ability to perform the requirements of the contract that are designated as operationally critical support.

Reporting a Cyber Incident

What is a cyber incident? **Actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein**

- **When DFARS Clause 252.204-7012 is included in a subcontract, subcontractors are required to rapidly report cyber incidents directly to DoD.**
  - **Subcontractors must also provide the incident report number, automatically assigned by DoD, to their prime Contractor as soon as practicable**

Where do contractors/subcontractors report?

- **DC3 is the single DoD focal point for receiving all cyber incident reporting affecting unclassified networks of DoD contractors**

All reporting will be via the Incident Collection Format (ICF) found at http://dibnet.dod.mil

Cyber Incident Damage Assessment Activities

> **DFARS 252.204-7012 (g) *Cyber incident damage assessment activities.* If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e)* of this clause.**
>
> ****(e) Media preservation and protection***

Purpose of damage assessment:

- **To understand impact of compromised information on U.S. military capability underpinned by technology**
- **Initiated after review of reported cyber incident**
- **Focused on determining impact of compromised intellectual property, not on mechanism of cyber intrusion**
- **An assessment is not possible without access to compromised material**

Safeguarding Covered Defense Information
What *IS* and is *NOT* Covered

- Scope of Clause: Applies to contracts/subcontracts requiring contractors/subcontractors to safeguard *covered defense information* that resides in/transits through covered systems
- Flowdown: The Contractor shall include Clause in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve a covered contractor information system…

What *Is* Covered?	**What is *Not* Covered?**
The contractor's internal information system(s)	**Government owned systems, systems operated on-behalf-of the government, military systems and facilities**
Req't for DoD to identify/mark covered defense information	**Changes to existing marking requirements for covered defense information, FOUO markings**
Security controls to safeguard covered defense information	**Verification, validation, certification or accreditation (e.g. RMF Authorization to Operate) of the contractor's system**
Single DoD focal point for receiving all incident reports	**Cyber incident reporting to any site other than *http://dibnet.dod.mil***

Contracting for Cloud Services

DFARS SUBPART 239.76 and DFARS Clause 252.239-7010

DFARS subpart 239.76, Cloud Computing:

- Implements policy developed by DoD CIO and the DoD Cloud Computing Security Requirements Guide (SRG)
- Directs use of DFARS Provision 252.239-7009, Representation of Use of Cloud Computing in solicitations for information technology services
  - Allows offeror to represent intention to utilize cloud computing services in performance of the contract or not.
- Directs use of DFARS Clause 252.239-7010, Cloud Computing Services in solicitations and contracts for information technology services
  - Provides standard contract language for the acquisition of cloud computing services, including access, security, and reporting requirements
  - Ensure uniform application of DoD's policies concerning Cloud Computing Services.

DFARS 252.239-7010(d) The Contractor shall report all cyber incidents that are related to the cloud computing service provided under this contract. Reports shall be submitted to the Department of Defense via http://dibnet.dod.mil/.

Contracting for Cloud Services

What IS and is NOT Covered

- Scope of Clause: Applies when using cloud computing to provide information technology services in the performance of the contract.
- Flowdown: The Contractor shall include the substance of the clause in all subcontracts that involve or may involve cloud services, including subcontracts for commercial items.

What *Is* Covered? **DoD Cloud Computing SRG applies**	**What is *Not* Covered?**
• **A cloud solution is being used to process data on the DoD's behalf**	• **A contractor uses his own internal cloud solution to do his processing related to meeting a DoD contract requirement to develop/deliver a product, i.e., as part of the solution for his internal contractor system.** – **Example: Contractor is developing the next generation tanker, and uses his internal cloud for the engineering design.** • **NIST SP 800-171 applies**
• **DoD is contracting with Cloud Service Provider to host/process data in a cloud**	
• **Cloud solution is being used for processing what we (the DoD) would normally do ourselves but have decided to outsource**	

What’s Next in the Rule Making Process

- The public comment period for the 1st interim rule (published Aug 26, 2015) closed on November 20, 2015
- The public comment period for the 2nd interim rule (published Dec 30, 2015) closed February 29, 2016
- All comments received will be considered in the formation of a single final rule
- DPAP, DoD CIO, and DASD(SE) are currently drafting the final rule

Resources

- DPAP Website/DARS/DFARS and PGI (http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html)
  - DFARS Subpart 204.73 and PGI 204.73 - Safeguarding Covered Defense Information and Cyber Incident Reporting
  - SUBPART 239.76 and PGI 239.76 – Cloud Computing
  - 252.204-7008 Compliance with Safeguarding Covered Defense Information Controls.
  - 252.204-7009 Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information
  - 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
  - 252.239-7009 Representation of Use of Cloud Computing
  - 252.239-7010 Cloud Computing Services
  - Frequently Asked Questions
- NIST SP 800-171 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf)
- Cloud Computing Security Requirements Guide (SRG) (http://iase.disa.mil/cloud_security/Documents/u-cloud_computing_srg_v1r1_final.pdf)

Resources Available to Industry

- United States Computer Emergency Readiness Team (US-CERT)
  http://www.us-cert.gov
- FBI InfraGard
  https://www.infragard.org
- DHS Cybersecurity Information Sharing and Collaboration Program (CISCP)
  https://www.dhs.gov/ciscp
- DHS Enhanced Cybersecurity Services (ECS)
  https://www.dhs.gov/enhanced-cybersecurity-services
- DoD's Defense Industrial Base Cybersecurity program (DIB CS program)
  http://www.dibnet.dod.mil
- Defense Security Information Exchange (DSIE)
  www.DSIE.org

Questions?